

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 1 de 20
---	--	---

1. Introducción

El Tecnológico de Antioquia – Institución Universitaria define su política del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión (MIPG) basada en la guía para la administración del riesgo vigente y el diseño de controles en entidades públicas que busca la articulación de los riesgos de gestión, corrupción, seguridad digital, riesgo fiscal y la estructura del Sistema Integrado de Gestión –SGI en lo relacionado con riesgos.

La política está compuesta por el objetivo, alcance, niveles de aceptación al riesgo, niveles para calificar el impacto, el tratamiento de riesgos, el seguimiento periódico según nivel de riesgo residual y responsabilidad de gestión para cada línea de defensa

Este documento busca definir los lineamientos para la adecuada gestión de los riesgos mediante la identificación de acciones institucionales ante las situaciones que puedan afectar el cumplimiento de la misión y el logro de objetivos institucionales, disminuyendo posibles consecuencias negativas, reduciendo la vulnerabilidad ante las amenazas y mejorando la capacidad de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad

2. Política de Administración de riesgos

Todos los procesos, niveles y áreas deben aplicar lineamientos que permitan la identificación, el análisis, la valoración y el tratamiento de los riesgos que pueden afectar la misión y el cumplimiento de los objetivos institucionales en el marco de los programas, proyectos, planes, procesos y productos mediante:

- a) La identificación y documentación de riesgos: de gestión (financiera, contractual, jurídico, académica, entre otros), riesgos de posibles actos de corrupción, los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad de seguridad digital en los programas, proyectos, planes y procesos; y riesgo fiscal.
- b) El establecimiento de acciones de control de detección y prevención para los riesgos identificados;
- c) La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

3. Objetivo

Alcanzar un nivel aceptable de riesgos residuales en todos los procesos, a través de la gestión de acciones de control, principios, directrices y responsabilidades para la implementación, mantenimiento y mejora continua del Sistema de Administración del Riesgo en el Tecnológico de Antioquia I.U con el fin de asegurar el cumplimiento de la misión institucional, los compromisos de gobierno, los objetivos estratégicos y de procesos vigentes.

 <p>TdeA Institución Universitaria</p>	<p>POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA</p>	<p>Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 2 de 20</p>
--	---	--

4. Alcance

La política aplica a la identificación, valoración, tratamiento y seguimiento de los riesgos de gestión, corrupción, seguridad digital y riesgo fiscal a todos los procesos, proyectos, servicios y planes de la entidad, conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa.

5. Términos y definiciones

- **Administración del Riesgo (Gestión del Riesgo):** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Implica la aplicación sistemática de políticas, procedimientos y prácticas para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos.

- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **Causa Raíz (Causa eficiente o causa Adecuada):** Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.

- **Control (Acción de Mitigación):** Medida preventiva, detectiva o correctiva implementada para modificar el riesgo, reduciendo su probabilidad de ocurrencia o su impacto.

- **Impacto (Consecuencia):** Resultado de la ocurrencia de un evento, que puede ser positivo o negativo. Se evalúa en términos de afectación a los objetivos de la Institución (financiero, reputacional, operacional, académico, legal, etc.).

- **Mapa de Riesgos:** Representación gráfica o tabular de los riesgos identificados en un proceso o en la entidad, clasificados según su probabilidad de ocurrencia y magnitud de impacto.

- **Monitoreo del Riesgo:** Proceso continuo de comprobación, supervisión, observación crítica o determinación del desempeño de la gestión del riesgo y la efectividad de los controles.

 <p>TdeA Institución Universitaria</p>	<p>POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA</p>	<p>Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 3 de 20</p>
--	---	--

- **Proceso:** Conjunto de actividades interrelacionadas o que interactúan, que transforman elementos de entrada en resultados. En el contexto universitario, incluye procesos misionales (académicos, investigación, extensión) y de apoyo (financieros, talento humano, tecnológicos).
- **Probabilidad:** Posibilidad de que un evento o situación específica ocurra.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado, positivo o negativo.
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo fiscal:** Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Efecto del riesgo fiscal: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento potencial el riesgo fiscal: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Tratamiento del Riesgo:** Proceso de modificación del riesgo. Implica la selección e implementación de una o más opciones para modificar los riesgos.

6. Metodología para la Administración del Riesgo

El Tecnológico de Antioquia I.U adoptará la metodología de administración del riesgo establecida en la Guía de Administración del Riesgo de Función Pública, la cual se fundamenta en la Norma Técnica Colombiana NTC-ISO 31000 de Gestión del Riesgo. Esta metodología consta de los siguientes pasos interrelacionados:

- **Establecimiento del contexto:** Definición del entorno interno y externo de la entidad, sus objetivos estratégicos y operacionales, y los criterios para la evaluación del riesgo.

- **Identificación de riesgos:** Proceso para encontrar, reconocer y describir los riesgos, incluyendo sus fuentes, eventos, causas y posibles consecuencias.
- **Análisis de riesgos:** Comprensión de la naturaleza del riesgo y sus características, incluyendo el nivel de probabilidad y la magnitud del impacto.
- **Valoración de riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos para determinar si un riesgo y/o su magnitud es aceptable o tolerable.
- **Tratamiento de riesgos:** Selección e implementación de opciones para modificar los riesgos. Esto puede incluir evitar el riesgo, tomar o incrementar el riesgo para buscar una oportunidad, eliminar la fuente del riesgo, cambiar la probabilidad, cambiar las consecuencias, compartir el riesgo o retener el riesgo.
- **Monitoreo y revisión:** Proceso continuo de seguimiento a la efectividad de los controles, identificación de nuevos riesgos o cambios en los existentes, y verificación del cumplimiento de los objetivos de la gestión del riesgo.
- **Comunicación y consulta:** Intercambio continuo de información sobre el riesgo entre todas las partes interesadas, internas y externas.

7. Niveles de Responsabilidades y autoridad

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:

Cuadro 1. Líneas de defensa del Tecnológico de Antioquia

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo	Periodicidad
Estratégica (Alta Dirección)	Comité de Gestión y Desempeño Institucional	<ul style="list-style-type: none">• Definir el marco general para la gestión del riesgo• Asegurar la implementación y desarrollo de las políticas de gestión y desempeño institucional que permitan apalancar la gestión del riesgo.	Anualmente revisará el marco general
	Comité institucional de coordinación de control interno CICCI	<ul style="list-style-type: none">• Aprobar la política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico y hacer seguimiento para su posible actualización.	<ul style="list-style-type: none">• Anual• La revisión del contexto se hará cuando se evidencien cambios en el entorno

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo	Periodicidad
		<ul style="list-style-type: none"> • Evaluar la eficacia de la política frente a la gestión del riesgo institucional. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles. • Realizar seguimiento y análisis periódico a los riesgos institucionales. 	
Primera Línea	Líderes de procesos y servidores en general	<ul style="list-style-type: none"> • Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera con énfasis en la prevención del daño antijurídico. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras a la gestión del riesgo en su proceso. • Reportar los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • Informar a la dirección de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo. • Reportar los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. • Analizar los resultados 	<p>Periodicidad para el monitoreo y revisión:</p> <p>El monitoreo de los riesgos y controles debe ser permanente y continuo, como parte integral de las operaciones diarias.</p> <p>La revisión formal de los riesgos y controles por parte de los responsables de proceso se realizará como mínimo de forma semestral o cuando ocurran eventos significativos que</p>

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo	Periodicidad
		del seguimiento y establecer acciones inmediatas ante cualquier desviación.	puedan afectar el perfil de riesgo.
Segunda línea	Dirección de Planeación	<ul style="list-style-type: none"> • Asesorar en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional. • Presentar al CICCI el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalúe y gestione los riesgos y controles para que se generen acciones. • Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. • Promover ejercicios de 	<p>Periodicidad para el monitoreo y revisión:</p> <p>La Dirección de Planeación realizará el monitoreo y consolidación del perfil de riesgo institucional de forma mensual, y presentará informes de seguimiento al Comité Institucional de Coordinación de Control Interno (CICCI) de forma semestral o cuando sea requerido.</p>

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo	Periodicidad
		<p>autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.</p> <ul style="list-style-type: none"> • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del comité institucional de coordinación de control interno 	
	Secretaría General, líderes de procesos de contratación, financiera, talento humano, gestión y defensa jurídica, TIC, servicio al ciudadano, comunicaciones, gestión del conocimiento y gestión documental y los supervisores de contrato de la Entidad entre otros	<ul style="list-style-type: none"> • Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo • Reportar a la Oficina de Planeación a través del SGI – módulo de riesgos, el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención del daño antijurídico • Supervisar que la primera línea de defensa identifique, evalúe y gestione los riesgos en los temas de su competencia 	
Tercera Línea	Oficina de Control interno	<ul style="list-style-type: none"> • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la 	Periodicidad para el monitoreo y revisión: La Oficina de Control Interno realizará auditorías de gestión del riesgo

 <p>TdeA Institución Universitaria</p>	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 8 de 20
--	--	---

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo	Periodicidad
		<p>segunda línea de defensa</p> <ul style="list-style-type: none"> • Asesorar de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI • Recomendar mejoras a la política de administración del riesgo 	de forma anual o según el plan de auditoría institucional, con la periodicidad que determine el plan de auditoría basado en el nivel de riesgo de cada proceso.

8. Herramienta para la Administración del Riesgo

El Tecnológico de Antioquia I.U utilizará como herramienta el Sistema de Gestión de la Calidad, el cual estará una hoja de cálculo centralizada el SIG, para el registro, seguimiento y monitoreo de los riesgos identificados.

Manejo de la herramienta:

- **Acceso:** El acceso a SIG estará restringido a los usuarios autorizados, con perfiles de acceso diferenciados según su rol y responsabilidad en la gestión del riesgo.
- **Registro:** Los responsables de proceso deberán registrar en la herramienta la identificación, análisis, valoración y tratamiento de los riesgos de sus procesos, incluyendo los controles establecidos.
- **Actualización:** La información de los riesgos y controles deberá mantenerse actualizada de manera permanente por los responsables de proceso.
- **Reportes:** La herramienta permitirá la generación de reportes y tableros de control para el monitoreo del perfil de riesgo institucional y la toma de decisiones.
- **Capacitación:** Se brindará capacitación periódica a los funcionarios sobre el uso adecuado de la herramienta.

9. Factores de riesgo estratégicos para la entidad

Los factores de riesgo estratégicos son aquellos que tienen el potencial de afectar significativamente

 <p>TdeA Institución Universitaria</p>	<p>POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA</p>	<p>Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 9 de 20</p>
--	---	--

el logro de los objetivos misionales y estratégicos del Tecnológico de Antioquia I.U. A partir de estos factores, todos los procesos deberán iniciar sus análisis para el establecimiento del contexto. Algunos de los factores de riesgo estratégicos a considerar son:

- **Factores políticos y regulatorios:** Cambios en políticas educativas, regulaciones gubernamentales, normativas de acreditación, estabilidad política y legal.
- **Factores económicos:** Restricciones presupuestarias, inflación, fluctuaciones económicas, disponibilidad de recursos financieros, sostenibilidad fiscal.
- **Factores sociales y demográficos:** Cambios en las tendencias demográficas, demanda de programas académicos, equidad e inclusión, movilidad social, percepción de la calidad educativa.
- **Factores tecnológicos:** Obsolescencia tecnológica, ciberseguridad, infraestructura tecnológica, nuevas herramientas pedagógicas, transformación digital.
- **Factores ambientales:** Impacto ambiental de las operaciones, normativas ambientales, eventos climáticos extremos.
- **Factores de competencia:** Análisis de resultados frente a otras instituciones de educación superior, oferta académica, calidad de la investigación.
- **Factores reputacionales:** Crisis de imagen, quejas y reclamos, resultados de auditorías, escándalos o situaciones que afecten la confianza pública.
- **Factores de capital humano:** Rotación de personal clave, escasez de talento, brechas de habilidades, clima laboral, ética y transparencia del personal.

10. Lineamientos para cada paso de la metodología

A continuación, se detallan los lineamientos específicos para cada paso de la metodología de administración del riesgo, con el fin de guiar a todos los procesos en sus análisis:

10.1 Establecimiento del contexto

- **Identificación de objetivos:** Cada proceso deberá identificar claramente sus objetivos, los cuales deben estar alineados con los objetivos estratégicos y misionales de la Institución.
- **Análisis del entorno:** Realizar un análisis DAFO (Debilidades, Amenazas, Fortalezas, Oportunidades) para comprender el entorno interno y externo del proceso.
- **Definición de criterios de riesgo:** Establecer los criterios para la evaluación del riesgo, incluyendo el apetito de riesgo de la entidad y los niveles de riesgo aceptado.

10.2 Identificación de Riesgos

- **Fuentes de riesgo:** Considerar fuentes internas (infraestructura, personal, procesos, tecnología) y externas (políticas públicas, mercado, sociedad, ambiente).

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 10 de 20
---	--	--

- **Clasificación de riesgos:** Clasificar los riesgos según su naturaleza (operacionales, estratégicos, financieros, tecnológicos, seguridad de la información, corrupción, etc.).
- **Técnicas de identificación:** Utilizar talleres, entrevistas, revisión documental, análisis de incidentes previos, y otras técnicas apropiadas para cada proceso.

10.3 Análisis de riesgos

- **Determinación de probabilidad e impacto:** Para cada riesgo identificado, estimar su probabilidad de ocurrencia y el impacto potencial en los objetivos de la entidad, utilizando las tablas institucionales de probabilidad e impacto.
- **Factores agravantes/atenuantes:** Identificar factores que puedan aumentar o disminuir la probabilidad o el impacto del riesgo.

10.4 Valoración de Riesgos

- **Nivel de riesgo Inherente:** Calcular el nivel de riesgo inherente (sin controles) utilizando la matriz de riesgo institucional
- **Comparación con criterios:** Comparar el nivel de riesgo inherente con los niveles de riesgo aceptado para la entidad.

10.5 Tratamiento de riesgos

- **Definición de controles:** Diseñar e implementar controles (preventivos, detectivos, correctivos) para mitigar los riesgos. Los controles deben ser proporcionales al nivel de riesgo y costo-efectivo.
- **Plan de acción:** Establecer planes de acción claros y responsables para la implementación de los controles.
- **Nivel de riesgo residual:** Calcular el nivel de riesgo residual (después de la implementación de controles) y asegurar que esté dentro de los niveles aceptados.
- **Estrategias de tratamiento:** Considerar opciones como evitar, reducir, compartir o aceptar el riesgo.

10.6 Monitoreo y revisión

- **Indicadores de gestión:** Definir indicadores clave de desempeño para el monitoreo de los riesgos y la efectividad de los controles.
- **Reporte periódico:** Realizar informes periódicos sobre el estado de los riesgos, los controles y las acciones correctivas.
- **Actualización del perfil de riesgo:** Actualizar el perfil de riesgo del proceso y de la entidad en general, identificando nuevos riesgos o cambios en los existentes.
- **Flujos de Información:** Establecer canales de comunicación claros para el intercambio de

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 11 de 20
---	--	--

información sobre riesgos entre los diferentes niveles y áreas de la entidad.

- **Participación:** Fomentar la participación de todos los funcionarios en la identificación y gestión de riesgos.

11. Niveles de riesgo aceptado y su forma de manejo

Acorde con los riesgos residuales aprobados por los líderes de procesos y socializados en el Comité Institucional de Coordinación de Control Interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

Para los riesgos residuales de gestión, seguridad digital y riesgos fiscales que se encuentren en zona de riesgo baja, está dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida, pero los que se encuentren en niveles de riesgo residual "medio, alto o extremo" requieren **acción inmediata** y se deberán formular e implementar planes de acción y controles específicos para mitigar, transferir, evitar o aceptar el riesgo.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

Es importante aclarar que, si un riesgo fiscal se materializa debido a un acto de corrupción, se le dará el tratamiento de "riesgo de corrupción" y no habrá aceptación del riesgo residual, debiendo siempre generar acciones de fortalecimiento y, si aplica, denuncias.

Contexto Estratégico

Se analiza periódicamente el contexto (las cuestiones internas y externas pertinentes para el análisis de riesgos), para establecer su complejidad, procesos y planeación institucional, entre otros aspectos, esto permite conocer y entender la entidad y su entorno. Es importante asegurar que el proceso de análisis del contexto se realice de forma continua y que los hallazgos se integren adecuadamente en la identificación y valoración de riesgos. Además, es de vital importancia revisar los cambios en el "Contexto Estratégico" y cómo estos pueden generar nuevos riesgos. Entre otras se analizan las siguientes variables:

INTERNO	EXTERNO
Financiero	Económicos y Financieros
Talento humano	Internacional
Procesos	Político
Tecnología	Social y cultural
Estratégicos	Tecnológico
Comunicación interna	Ambiental
Infraestructura	Legal
Diseño del proceso	Comunicación externa

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01
		Versión: 01
		Fecha de Aprobación: Mayo 12 de 2025
		Página 12 de 20

INTERNO	EXTERNO
Interacción con otros procesos Procedimientos asociados Responsables del proceso Comunicación entre los procesos Seguridad digital Social y cultural Seguridad y salud en el trabajo Ambiental Reputacional	Evento externo

12. Tablas de probabilidad e impacto institucional.

Nivel de calificación de probabilidad para riesgos de proceso, fiscal y seguridad de la información

Nivel	Probabilidad	Descripción
100%	Muy Alta	La actividad se realiza más de 5001 veces al año.
80%	Alta	La actividad se realiza entre 501 a 5000 veces al año.
60%	Media	La actividad se realiza entre 25 a 500 veces al año
40%	Baja	La actividad se realiza entre 3 a 24 veces al año.
20%	Muy Baja	La actividad se realiza máximo 2 veces al año

Nivel de calificación de probabilidad para riesgos de corrupción

Nivel	Probabilidad	Probabilidad	Descripción
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año
3	Possible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

Niveles de calificación de impacto

La calificación del impacto para los riesgos de gestión y de seguridad de la información se tendrá

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01
		Versión: 01
		Fecha de Aprobación: Mayo 12 de 2025
		Página 13 de 20

en cuenta la siguiente escala, de acuerdo con la realidad de Función Pública.

Tabla 5. Calificación de impacto para riesgos de proceso, fiscal y seguridad digital

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
100%	Catastrófico	Pérdida económica superior a 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel internacional.
80%	Mayor	Pérdida económica de 319 hasta 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial.
60%	Moderado	Pérdida económica de 21 hasta 318 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos.
40%	Menor	Pérdida económica de 11 hasta 20 SMLV	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
20%	Leve	Pérdida económica hasta 10 SMLV	Solo de conocimiento de algunos funcionarios.

La calificación del impacto para los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 6. Calificación del Impacto para los riesgos de corrupción

No.	Si el riesgo de corrupción se materializa podría	Respuesta	
		Sí	No
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01
		Versión: 01
		Fecha de Aprobación: Mayo 12 de 2025
		Página 14 de 20

No.	Si el riesgo de corrupción se materializa podría	Respuesta	
		Sí	No
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasional lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Nivel	Descriptor	Descripción	Respuestas afirmativas
1	Moderado	Genera medianas consecuencias sobre la entidad	1 a 5
2	Mayor	Genera altas consecuencias sobre la entidad	6 a 11
3	Catastrófico	Genera consecuencias desastrosas para la entidad	12 a 19

13. Accionar ante los riesgos materializados

Ante la materialización de un riesgo se deberá medir el impacto y las consecuencias que puede ocasionar afectaciones a los objetivos de la Entidad, se revisarán y ajustarán los controles asociados determinando el grado de efectividad, eficiencia o eficacia, que garantice la mitigación de la ocurrencia. Para adelantar el análisis del riesgo y sus controles se deben considerar los siguientes aspectos:

- Calificación del riesgo: se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.
- Bajo el criterio de probabilidad: el riesgo se debe medir a partir de la cantidad de veces que se ejecuta cada una de sus acciones

Se deberán tomar las medidas encaminadas a prevenir la ocurrencia como primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de ajustes en los controles y acciones emprendidas.

El accionar ante los riesgos, define el cómo ejecutar, proceder y realizar una acción paso a paso o de manera secuencial en un evento, acontecimiento o hecho determinado. Se definen las acciones a tomar una vez se compruebe la materialización de un riesgo según se describe en el siguiente cuadro.

Tipo de Riesgo	Acción
----------------	--------

	<p><u>Líder del proceso</u></p> <ul style="list-style-type: none"> • Informar al área de Planeación sobre el hecho encontrado. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. • Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Actualizar el mapa de riesgos. <p><u>Oficina de Control interno</u></p>
Riesgo Corrupción de	<ul style="list-style-type: none"> • Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado). • Realizar la denuncia ante la instancia de control correspondiente.
Riesgos Gestión, de seguridad digital y riesgos de riesgos fiscales	<p><u>Líder del proceso</u></p> <p>Informar al área de Planeación sobre el hecho encontrado</p> <p>Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento de este (si es el caso), documentar en el Plan de mejoramiento.</p> <p>Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de Mejoramiento Institucional y replantear los riesgos del proceso.</p> <p>Analizar y actualizar el mapa de riesgos.</p> <p>Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.</p> <p>Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.</p> <p><u>Oficina de Control interno</u></p> <ul style="list-style-type: none"> • Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar • Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho. • Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

14. Manejo del Riesgo Fiscal

El Tecnológico de Antioquia incorporará el manejo del riesgo fiscal como parte integral de su sistema de administración del riesgo. Para ello, se tendrán en cuenta los siguientes lineamientos:

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 16 de 20
---	--	--

- **Identificación:** Identificar los riesgos asociados a la gestión de los recursos públicos, tales como desviaciones presupuestarias, ineficiencia en el gasto, incumplimiento de metas fiscales, debilidades en la ejecución presupuestal, etc.
- **Análisis y Valoración:** Analizar la probabilidad e impacto de los riesgos fiscales, considerando la normatividad vigente y las directrices de los entes de control fiscal.
- **Tratamiento:** Diseñar e implementar controles específicos para mitigar los riesgos fiscales, como el establecimiento de topes de gasto, el seguimiento a indicadores de gestión financiera, la optimización de procesos de contratación, la implementación de planes de saneamiento fiscal, etc.
- **Monitoreo y Reporte:** Realizar un seguimiento periódico al perfil de riesgo fiscal y reportar a la alta dirección y a los entes de control, según lo establecido en la normatividad aplicable.

15. Riesgos relacionados con posibles actos de corrupción

El Tecnológico de Antioquia I.U promoverá la cultura de la legalidad y la transparencia, incorporando la gestión de los riesgos de corrupción como un pilar fundamental. Los lineamientos son:

- **Identificación:** Identificar los puntos críticos en los procesos donde pueden materializarse actos de corrupción (contratación, gestión de personal, trámites administrativos, gestión de bienes, etc.).
- **Análisis y Valoración:** Evaluar la probabilidad e impacto de los riesgos de corrupción, considerando factores como la discrecionalidad en la toma de decisiones, la falta de controles, la concentración de poder, etc.
- **Tratamiento:** Implementar medidas preventivas (códigos de ética, políticas de buen gobierno, programas de formación, canales de denuncia anónimos) y detectivas (auditorías forenses, monitoreo transaccional, revisión de conflictos de interés) para mitigar estos riesgos.
- **Cultura Organizacional:** Fomentar una cultura de cero tolerancias a la corrupción, promoviendo valores de integridad y ética en todos los niveles de la entidad.

16. Riesgos laborales

Los riesgos laborales son todas aquellas situaciones, condiciones o elementos presentes en un entorno de trabajo que pueden causar daños a la salud, la seguridad o el bienestar de los trabajadores, en este caso los servidores públicos, los estudiantes y los contratistas que prestan servicios personales al TdeA. Estos riesgos pueden derivar en accidentes, incidentes, enfermedades profesionales u otros problemas físicos o psicológicos.

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 17 de 20
---	--	--

Clasificación de los riesgos laborales

Se suelen clasificar en cinco grandes grupos:

1. Riesgos físicos: relacionados con factores del entorno como ruido, vibraciones, temperaturas extremas, radiaciones, etc.
2. Riesgos químicos: exposición a sustancias peligrosas como gases, vapores, líquidos tóxicos, polvo, etc.
3. Riesgos biológicos: exposición a virus, bacterias, hongos u otros organismos vivos.
4. Riesgos ergonómicos: derivados de una mala postura, movimientos repetitivos, manipulación de cargas, etc., que pueden causar trastornos músculo-esqueléticos.
5. Riesgos psicosociales: relacionados con la organización del trabajo, como el estrés, la presión excesiva, el acoso laboral, la falta de apoyo, etc.

Para el tratamiento de estos riesgos se determinan instrumentos que garantizan la sujeción de la institución a las normas y reglamentos que sobre el Sistema de Gestión de Seguridad y Salud en el Trabajo determine el Gobierno Nacional.

17. Riesgos biológicos y químicos

Los riesgos biológicos, son aquellos riesgos que provienen de organismos vivos o de sus productos, y que pueden causar efectos adversos para la salud humana, animal o el medio ambiente, estos riesgos pueden estar presentes en el TdeA en entornos de aprendizaje como laboratorios, huertas o en actividades relacionadas con la biotecnología o la agricultura.

Los principales agentes biológicos que representan un riesgo son:

- Bacterias
- Virus
- Hongos
- Parásitos

De otro lado, los riesgos químicos son aquellos peligros que provienen del uso, manipulación o exposición a sustancias químicas que pueden afectar la salud de las personas, causar daños materiales o contaminar el medio ambiente, estos riesgos están presentes en entornos propios de la academia, tales como laboratorios, espacios para la agricultura y la limpieza de espacios.

Los tipos de riesgos químicos (según el efecto que producen), son:

- Tóxicos: Pueden causar envenenamiento o daño a órganos
- Corrosivos: Destruyen tejidos vivos o materiales
- Irritantes: Causan inflamación o molestias en piel, ojos o vías respiratorias

 <p>TdeA Institución Universitaria</p>	<p>POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA</p>	<p>Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 18 de 20</p>
--	---	---

- Inflamables: Se encienden fácilmente al contacto con una fuente de calor
- Explosivos: Liberan energía súbitamente al descomponerse (Ej. nitrato de amonio).
- Carcinógenos: Pueden causar cáncer con la exposición prolongada
- Mutagénicos y teratogénicos: Afectan el ADN o el desarrollo fetal

Vías de entrada al cuerpo:

- Inhalación: Vapores, gases, polvos o aerosoles.
- Absorción: A través de la piel o los ojos.
- Ingestión: Por alimentos o manos contaminadas.
- Inyección: Accidental o intencional

El TdeA administra este tipo de riesgos de acuerdo con el grado de exposición y los ambientes de aprendizaje donde se desarrollen actividades que puedan ser causa o agentes generadores, por lo que, cada espacio (laboratorio, granja, aula, etc.), cuenta con su respectivo Manual de Bioseguridad, en el cual se incluye la identificación de los riesgos que le son propios y registra los protocolos de atención, en caso de materializarse o de presentarse el incidente generador.

10.3. Anexo metodológico para la Gestión de Riesgos de Seguridad de la Información

El Tecnológico de Antioquia I.U adoptará el Anexo Metodológico para la Gestión de Riesgos de Seguridad de la Información de la Guía de Administración del Riesgo de Función Pública, y lo complementará con las directrices de la Norma Técnica Colombiana ISO/IEC 27001 de Sistemas de Gestión de la Seguridad de la Información. Los aspectos clave incluyen:

- **Identificación de Activos:** Identificar y clasificar los activos de información (datos, sistemas, infraestructura, software) según su criticidad.
- **Identificación de amenazas y vulnerabilidades:** Identificar las amenazas (ataques cibernéticos, fallas de hardware, errores humanos) y las vulnerabilidades (sistemas desactualizados, falta de capacitación, configuraciones inseguras) que pueden afectar la confidencialidad, integridad y disponibilidad de la información.
- **Análisis y valoración:** Evaluar el riesgo de seguridad de la información, considerando la probabilidad de materialización de las amenazas y el impacto en los activos de información.
- **Tratamiento:** Implementar controles técnicos (firewalls, cifrado, sistemas de detección de intrusos), organizacionales (políticas de seguridad, roles y responsabilidades), y físicos (seguridad de los centros de datos) para mitigar los riesgos de seguridad de la información.
- **Gestión de Incidentes:** Establecer procedimientos claros para la gestión de incidentes de seguridad de la información, incluyendo la detección, respuesta y recuperación.

11. Otros aspectos considerados necesarios

	POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA	Código: OT-DEP-01 Versión: 01 Fecha de Aprobación: Mayo 12 de 2025 Página 19 de 20
---	--	--

- **Cultura de Gestión del Riesgo:** Promover una cultura organizacional que entienda y valore la gestión del riesgo como una herramienta para el mejoramiento continuo y el logro de objetivos. Se realizarán jornadas de sensibilización y capacitación periódicas.
- **Articulación con la planeación Estratégica:** La identificación y tratamiento de riesgos se articulará directamente con el ciclo de planeación estratégica de la entidad, asegurando que los riesgos se consideren en la formulación de objetivos y metas.
- **Revisión periódica de la política:** Esta política será revisada y actualizada anualmente o cuando existan cambios significativos en la normatividad, el contexto institucional o los resultados de la gestión del riesgo.
- **Roles y responsabilidades claros:** Se asegurará que todos los funcionarios comprendan sus roles y responsabilidades en la gestión del riesgo a través de la comunicación efectiva y la capacitación continua.
- **Mejora continua:** Se establecerán mecanismos para la mejora continua del sistema de administración del riesgo, a partir de los resultados de las auditorías internas y externas, las evaluaciones de desempeño y las lecciones aprendidas de los incidentes de riesgo.



POLÍTICA DE GESTIÓN DEL RIESGO DEL TECNOLÓGICO DE ANTIOQUIA

Código: OT-DEP-01
Versión: 01
Fecha de Aprobación:
Mayo 12 de 2025
Página 20 de 20

Anexos

Matriz de gestión de riesgos y controles

Formato materialización del riesgo

Matriz de riesgo institucional